I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

FISA Reform

LAURA K. DONOHUE*

I. INTRODUCTION

On October 4, 2001, President Bush authorized the National Security Agency (NSA) to collect two different types of bulk information: telephony and Internet metadata, and telephone and Internet content.[1] The former gave the NSA the ability to identify

---

* Professor of Law, Georgetown Law. This Article constitutes the third section of a three-part series on NSA surveillance under FISA. *See* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, HARV. J. L. & PUB. POL'Y (2014); Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content* (2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436418.

[1] *Authorization for Specified Electronic Surveillance Activities During a Limited Period to Detect and Prevent Acts of Terrorism Within the United States*, Oct. 4, 2001, *cited in* OFFICE OF THE INSPECTOR GENERAL, NATIONAL SECURITY AGENCY CENTRAL SECURITY SERVICE, WORKING DRAFT ST-09-0002(Mar. 24, 2009)1, 7–8, 11, 15, *available at* http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection [hereinafter WORKING DRAFT]; The Obama Administration has publicly confirmed the inclusion of Internet and telephony metadata, and telephony content, as part of the President's Surveillance Program (PSP), but not Internet content. *See* Press Release, Director of National Intelligence, (DNI) Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001 (Dec. 21, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/991-dni-announces-the-declassification-of-the-exisitence-of-collection-activities-authorized-by-president-george-w-bush-shortly-after-the-attacks-of-september-11, 2001 [hereinafter Declassification Press Release]; Unclassified Declaration of Frances J. Fleisch, National Security Agency, Jewel v. NSA, No. 08-cv-4373-JSW (N.D. Cal. Dec. 20, 2013), *available at* https://www.eff.org/files/2013/12/21/fleisch2013jewelshubert.pdf (using language identical to DNI press release)[hereinafter Fleisch Declaration]. *See also* OLC-132, Memorandum from a Deputy Assistant Attorney General in the Office of Legal Counsel to the counsel to the President, regarding a request from the White House for OLC's views regarding what legal standards might govern the use of certain intelligence methods to monitor communications by potential terrorists, Oct. 4, 2001, *noted by* Second Redacted

terrorist-related activity through contact chaining—i.e., the process of building a network graph that modeled communication patterns of targets and their associates[2]—he latter provided raw intelligence.[3] Within a month, the President's Surveillance Program (PSP), renewed thereafter at 30-60 day intervals, became operational.[4]

Over the next twelve years, the contours of—and the legal basis for—the classified program and its component parts shifted. The Administration initially grounded PSP in the President's Article II Commander-in-Chief authorities, the 2001 Authorization for the Use of Military Force (AUMF), and the War Powers Resolution.[5] Gradually, key portions of the program were either eliminated or moved to the Foreign Intelligence Surveillance Act (FISA).[6] Critical statutory changes contributed to the process.[7] Despite these changes,

---

Declaration of Steven G. Bradbury, Elec. Priv. Info. Ctr. v. Dep't of Justice, 511 F. Supp. 2d 56 (D.D.C. 2007), *available at* https://www.aclu.org/sites/default/files/pdfs/safefree/aclu_v_doj_2nd_declaration_steven_bradbury.pdf.

2 WORKING DRAFT, *supra* note 1, at 13.

3 *Id.* at 15.

4 WORKING DRAFT, *supra* note 1, at 11 ("Within 30 days, the PSP was fully operational....Private sector partners began to send telephony and Internet content to NSA in October 2001. They began to send telephony and Internet metadata to NSA as early as November 2001").

5 *See, e.g.*, President's Radio Address, THE WHITE HOUSE, Dec. 17, 2005, *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051217.html; U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT (Jan. 19, 2006), *available at* http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf; Letter from William E. Moschella, Assistant Attorney General to The Hon. Pat Roberts, Chair, Senate Select Committee on Intelligence, The Hon. John D. Rockefeller, Vice Chairman, Senate Select Committee on Intelligence, The Hon. Peter Hoekstra, Chairman, Permanent Select Committee on Intelligence, U.S. House of Representatives, and the Hon. Jane Harman, Ranking Minority Member, Permanent Select Committee on Intelligence, U.S. House of Representatives (Dec. 22, 2005), *available at* https://www.fas.org/irp/agency/doj/fisa/doj122205.pdf.

6 *See* Foreign Intelligence Surveillance Act, Pub. L. No. 110-261, § 702, 122 Stat. 2436, codified at 50 U.S.C. § 1881 (2006). *See also* discussion, Part II, *infra*.

7 *See* Protect America Act of 2007, Pub. L. No. 110-55, § 2, 121 Stat. 553. (Aug. 5, 2007) (amending FISA, § 105B(a)(1)-(5)), codified at 50 U.S.C. § 1805b (2006)); FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (July 10, 2008).

calls for reform of FISA persisted.[8] For the most part, however, they met with little success.

It was not until Edward Snowden's releases, in June 2013 *et seq.*, the court-ordered release of documents in a Freedom of Information Act (FOIA) case, and the declassification of additional documents by the Obama Administration, that calls for significant reform took hold.[9] With FISA considered by Congress to be the sole means via which intelligence agencies could collect information on U.S. persons within the United States, attention was drawn to the legal sufficiency of the programs under the statute and the First and Fourth Amendments, and ways in which the legislative language could be altered to take account of new and emerging technologies, the needs of the intelligence community, civil liberties, and citizens' constitutional right to privacy. Dozens of reform initiatives are now on the table. The Administration has indicated a willingness to work with Congress to alter the statutory framing, and the legislature is poised to take up the issue of FISA reform.

What has been missing from the discussion is a comprehensive view of ways in which reform could be given effect—i.e., a taxonomy of potential reform efforts. This Article seeks to fill the gap. The aim is to deepen the conversation about potential approaches to foreign intelligence gathering, to allow fuller discussion of what a comprehensive reform package could contain, and to place specific reforms that are currently being advocated within a broader, over-arching framework.

The Article begins by addressing (to the extent that the information is publicly available) the legal underpinnings of PSP and

---

[8] For thoughtful and important contributions to FISA reform following the FAA, *see* William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEXAS L. REV. 1633 (2010); David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act: Progress to Date and Work Still to Come*, in LEGISLATING THE WAR ON TERROR: AN AGENDA FOR REFORM, 217 (Benjamin Wittes, ed., 2009); Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245 (2008); Orin S. Kerr, *Updating the Foreign Intelligence Surveillance Act*, 75 U. CHI. L. REV. 225 (2010); Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, U. CHI. L. REV. 287 (2008).

[9] *See, e.g.*, Elec. Frontier Found. v Dep't of Justice, No. 4:11-cv-05221-YGR (N.D. Cal. 2013); Declassification Press Release, *supra* note 1. *See also* Aamer Madhani, *DNI Releases More Documents to Justify NSA Surveillance*, USA TODAY, Dec. 21, 2013, http://www.usatoday.com/story/news/politics/2013/12/21/dni-nsa-documents-bulk-data/4157877/ ("In the face of growing skepticism over the National Security Agency's practice of collecting bulk phone and Internet records, the director of national intelligence on Saturday declassified several documents detailing the program. The latest declassification of documents comes during a week in which a federal judge ruled the NSA's bulk collection was likely unconstitutional and a White House task force questioned the effectiveness of the program.").

its progeny. It outlines the components of the original program and their transfer to FISA. Part II ends with an overview of the state of play with regard to current calls for reform.

Part III focuses on how technology has altered the types of information available, as well as methods of transmission and storage. It suggests that we now find ourselves in a world in which five primary types of information are available: personal, transactional, relational, locational, and content. Set against the five categories are six methods of access, transmission, and storage: audio/visual observation, communications networks, papers, hard drives and independent electronic devices, remote servers and cloud technologies, and social media. The purpose of this discussion is to step back from how foreign intelligence has traditionally been conceived, to consider the world as we now find it.

Part IV builds on the previous section by developing a taxonomy for how a statutory approach to foreign intelligence gathering could be given force. It divides foreign intelligence gathering into two categories: front-end collection and back-end analysis and use. Each category contains a counterpoise structured to ensure the appropriate exercise of Congressionally-mandated authorities. For the front-end, this means balancing the manner of collection with requirements for approval. For the back-end, this means offsetting implementation with transparency and oversight.

The taxonomy sub-divides for both parts of each category. The first half of the front-end framework, the manner of collection, proposes six sections. The first two divisions draw from Part III, emphasizing (1) the disparate types of information available and (2) distinct methods of access, transmission, and storage. To this are added (3) the form in which information is transferred, (4) the agency obtaining the information, (5) the target about whom information is sought, (6) the source of the data, and (7) the location of the material.

The second half of the front-end framework, requirements for approval, looks at four areas: (1) the entity approving the collection of information, (2) how this entity is constructed, (3) the scope of the approval, (4) verification, and (5) potential emergency exceptions.

Turning to the back-end framework, the Article addresses implementation as manifest through (1) analysis, (2) use, (3) retention, and (4) transfer of information. The second half of the back-end, transparency and oversight, emphasizes (1) who reports, (2) what is reported, (3) to whom such reports are made, (4) penalties for violations, and (5) alternative reporting channels.

Part V concludes by noting that the purpose of building the typology is to provide a framework for different considerations to be taken into account in constructing a comprehensive reform package. This Article does not take a substantive position on the categories put

forward. Instead, it identifies potential ways to proceed in developing an approach to foreign intelligence gathering that is cognizant of new and emerging technologies, as well as other, competing needs, such as intelligence gathering, threat assessments, economic stability, civil liberties, the right to privacy, and protections against the misuse of information.

II. LEGAL UNDERPINNINGS

From the beginning, information about the existence of, and the legal basis for, the PSP was tightly controlled.[10] Subjected to broader scrutiny, PSP's legal grounding altered. Eventually, the constituent portions of PSP were either eliminated or transferred to FISA's overarching framework. As more information became public, statutory and constitutional concerns emerged. Central to the debate has been the sufficiency of the existing statutory language in light of new and emerging technologies and the First and Fourth Amendment implications of the current programs. Resultantly, calls for reform are gaining ground.

A. *The President's Surveillance Program and its Transfer to FISA*

In March 2004, a classified review of the program by the Office of Legal Counsel (OLC) determined that there was legal support for three of the four types of collection included in PSP: (a) bulk telephony metadata, and the contents of (b) telephone and (c) Internet communications. OLC found that, in contrast to the three programs, the bulk Internet metadata collection appeared to be prohibited by the terms of FISA and Title III.[11] Based on OLC's finding, President George W. Bush rescinded the authority to collect bulk Internet

---

[10] *See, e.g.*, WORKING DRAFT, *supra* note 1, at 22 ("As directed by the White House, access to the original Presidential authorization and subsequent renewals was tightly controlled."); *Id.* at 21 (noting that "The NSA did not have access to the early DOJ Office of Legal Counsel (OLC) opinions supporting the Attorney General's statement that the PSP was legal."); Memorandum from George W. Bush, the White House, to the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Director of Central Intelligence, the Director of Federal Bureau of Investigation of Investigation, Re: Disclosures to the Congress (Oct. 5, 2001), *available at* http://www.fas.org/sgp/bush/gwb100501.html (directing members of the Cabinet to limit any disclosures to Congress regarding classified or sensitive law enforcement information to the Gang of Eight). *See also* WORKING DRAFT, *supra* note 1, at 25 (noting briefings only to the Gang of Eight).

[11] OLC apparently issued three opinions on this matter: Mar. 15, 2004, May 6, 2004, and July 16, 2004. WORKING DRAFT, *supra* note 1, at 37.

metadata and gave the NSA one week to terminate the program. Department of Justice and the NSA subsequently transferred the process to FISA's Pen Register/Trap and Trace Provisions (PRTT), with the first order approved July 14, 2007 and renewed thereafter at 90-day intervals.[12] The program appears to have operated until December 2011, when it was discontinued for failure to deliver sufficient operational value to the NSA.[13]

The three remaining PSP programs reviewed by OLC (bulk telephony metadata, and the contents of international telephone and Internet communications) appear to have been known only to a small number of people within the executive branch. It was not until a *New York Times* article was published in December 2005 that their existence reached the public domain.[14] At that time, only a narrow part of PSP emerged: the NSA's interception of (at least some) telephone content between the United States and overseas.[15] Some months later, the media reported further on the collection of domestic telephony metadata.[16]

Pressed in late 2005 and early 2006 for the legal rationale behind the interception of international communications, a program that the Administration referred to as the Terrorism Surveillance Program (TSP), the government cited the President's constitutional authorities

---

[12] WORKING DRAFT, *supra* note 1, at 38, 39; Declassification Press Release, *supra* note 1; Fleisch Declaration, *supra* note 1.

[13] *See* Declassification Press Release, *supra* note 1; Fleisch Declaration, *supra* note 1.

[14] James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers without Courts*, N.Y. TIMES, Dec. 16, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0 ("Months after the Sept. 11 attacks, President Bush secretly authorized the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying, according to government officials."). *See also* Eric Lichtblau and James Risen, *Spy Agency Mined Vast Data Trove*, Officials Report, N.Y. TIMES, Dec. 24, 2005, http://www.nytimes.com/2005/12/24/politics/24spy.html?pagewanted=all ("The National Security Agency has traced and analyzed large volumes of telephone and Internet communications flowing into and out of the United States as part of the eavesdropping program that President Bush approved after the Sept. 11, 2001, attacks to hunt for evidence of terrorist activity, according to current and former government officials.").

[15] Lichtblau and Risen, *Spy Agency Mined Vast Data Trove*, *supra* note 14.

[16] Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, *available at* http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm. *See also* Seymour M. Hersh, *Listening In*, NEW YORKER, May 29, 2006, *available at* http://www.newyorker.com/archiva/2006/05/29/060529ta_talk_hersh.

as Commander-in-Chief, the 2001 Authorization for the Use of Military Force (AUMF), and the War Powers Resolution (WPR).[17]

Congress and others offered three principal legal objections. First, that the legislature had intended the 1978 Foreign Intelligence Surveillance Act, which restricted electronic surveillance and required judicial approval for the granting of orders, to be the sole means via which the executive branch could conduct domestic surveillance for foreign intelligence and international counter-terrorism purposes.[18] FISA contemplated the advent of war, allowing a 15-day grace period, at the expiration of which the statute's provisions would be in effect.[19]

Second, while the AUMF gave the President the authority to "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks," neither the legislative history nor the text of the 2001 AUMF made explicit reference to electronic surveillance.[20]

Third, Congress (and the Courts) had previously considered and declined to recognize claims to Article II authority to conduct foreign

---

[17] *See, e.g.*, President's Radio Address, THE WHITE HOUSE, Dec. 17, 2005, *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051217.html; U.S. DEP'T OF JUSTICE, *supra* note 5; Letter from William E. Moschella, *supra* note 5.

[18] During passage of FISA, some members of the House of Representatives wanted the statute to read that it was the "exclusive statutory" means for the Executive to conduct electronic surveillance, implying in the process that the President had inherent surveillance powers outside the statute. The Senate rejected this notion, suggesting that if the President were to engage in electronic surveillance outside the parameters of FISA, on judicial review, they wanted the Supreme Court to treat the President's actions as under Justice Jackson's third category in *Youngstown*: against the expressed intent of Congress. The Senate view carried. *See* 50 U.S.C. §1811 et seq.

[19] 50 U.S.C. §1811 (2006) (electronic surveillance); 50 U.S.C. §1829 (2006) (physical search), 50 U.S.C. §1844 (2006) (pen/trap) ("Notwithstanding any other law, the President, through the Attorney General, may authorize [electronic surveillance, physical search, or pen/trap] to acquire foreign intelligence information for a period not to exceed 15 calendar days following a declaration of war by Congress."). It provided for a 15-day grace period, to "allow time for consideration of any amendment to [FISA] that may be appropriate during a wartime emergency." H.R. REP. NO. 95-1720, at 34 (1978) (Conf. Rep.), *reprinted in* 1978 U.S.C.C.A.N. 4048, 4063. At the expiry of the 15 days, absent any amendment, ordinary FISA provisions would have to be followed. Congress recognized that this had been a carefully-constructed compromise position: during the debates on FISA, the House of Representatives had sought a complete abatement of FISA during periods of declared war. The Senate objected, and the House of Representatives changed its position.

[20] Authorization for the Use of Military Force (AUMF), Pub. L. No. 107-40, § 2(a), 115 Stat. 224 (2001).

intelligence gathering within domestic bounds absent a warrant—this had been the basis on which FISA had been introduced.[21]

In the face of mounting public pressure, a company providing telephony metadata expressed concern to the NSA about the voluntary nature of the program, requesting that the process be, instead, one of government compulsion.[22] Resultantly, on May 24, 2006, the NSA transferred the bulk collection of telephony metadata to FISA's tangible goods provisions in Section 501 (as amended by USA PATRIOT Act Section 215).[23]

The remaining PSP collection programs, which focused on international telephone and Internet content, could not so easily be transferred to FISA.[24] To do so, DOJ and NSA would have to find a legal theory to support the NSA's addition and withdrawal of thousands of foreign targets for content collection.[25]

The solution ultimately turned on a new definition of "facility"—no longer would it be understood in relation to a particular telephone number or email address, but instead, it became defined in a manner that included general gateways used for communications.[26] In January

---

[21] In 1972, the Court held that government officials were obliged to obtain a warrant prior to electronic surveillance, even where domestic security might be on the line. The court cited the "inherent vagueness of the domestic security concept" and the potential for abuse and the targeting of political dissenters, to underscore the importance of Fourth Amendment protections. United States v. U.S. Dist. Court, 407 U.S. 297 (1972).

[22] WORKING DRAFT, *supra* note 1, at 39–40.

[23] USA PATRIOT Act, Sec. 215, amending FISA Sec. 501, codified at 50 USC §1861 (Access to certain business records for foreign intelligence and international terrorism investigations). For the original order for Verizon, *see In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Telecommunications Providers] Relating to [REDACTED], Order, No. BR-05 (FISA Ct. May 24, 2006), *available at* https://www.eff.org/sites/default/files/filenode/docket_06-05_1dec201_redacted.ex_-_ocr_0.pdf (released by court order as part of the Electronic Frontier Foundation's FOIA litigation). Note that the specific telecommunications company from which such records were sought were redacted, as well as the remaining title; however, the government also released an NSA report that provided more detail on the title of the Order. OFFICE OF THE INSPECTOR GEN., NAT'L SEC. AGENCY/CENT. SEC. SERV., ST-06-0018, REPORT ON THE ASSESSMENT OF MANAGEMENT CONTROLS FOR IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE COURT ORDER: TELEPHONY BUSINESS RECORDS (Sept. 5, 2006) (see page 94 of 1846 and 1862 Production, Mar. 5, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf.

[24] Telephone content collection came to be known as the Terrorism Surveillance Program.

[25] WORKING DRAFT, *supra* note 1, at 40.

[26] WORKING DRAFT, *supra* note 1, at 41.

2007, FISC approved the new theory with regard to foreign selectors but rejected it for the domestic realm, signing two separate orders.[27]

The former change immediately and negatively affected the number of foreign selectors that could be used with regard to collection.[28] It also placed a higher administrative burden on the NSA. In April 2007, the Director of National Intelligence, J.M. McConnell, submitted a proposal to Congress to amend FISA to make it easier for the executive branch to target U.S. interests abroad.

Four months later, Congress passed the Protect America Act (PAA), easing restrictions on the surveillance of foreigners where one (or both) parties were located overseas.[29] The statute removed the Foreign Intelligence Surveillance Court (FISC) from supervising the interception of communications that began or ended in a foreign country. In its place, the Attorney General and the Director of National Intelligence could authorize, up to one year, the acquisition of communications concerning "persons reasonably believed to be outside the United States," where five criteria were met.[30] The PAA required the Attorney General to submit the targeting procedures to FISC and to certify that the communications to be intercepted were not purely domestic in nature.[31] Once certified, FISC was required to

---

[27] Foreign Content Order, Jan. 10, 2007 and Domestic Content Order, Jan. 10, 2007, *cited in* WORKING DRAFT, *supra* note 1, at 41-42. For additional sources noting the ending of PSP in January 2007 *see also* S. REP. NO. 110-209, at 4 (2007); Letter from Attorney General Alberto Gonzales to Senate Judiciary Committee Chairman Patrick Leahy and Senator Arlen Specter (Jan. 17, 2007). Other documents, however, suggest that TSP transitioned to FISA in January 2007. *See, e.g.*, Declassification Press Release, *supra* note 1; Fleisch Declaration, *supra* note 1.

[28] Unlike the Foreign Content Order, the Domestic Content Order issued by FISC in January 2007 did not have an immediate, dramatic impact on collection. Nevertheless, it retarded the process to the point where, by January 2009, only a single selector was directed towards collection. The FBI subsequently took responsibility for the domestic order before the FISC. WORKING DRAFT, *supra* note 1, at 42.

[29] Protect America Act of 2007, Pub. L. No. 110-55, § 2, 121 Stat. 553 (Aug. 5, 2007) (amending FISA, § 105B(a)(1)-(5)), codified at 50 U.S.C. § 1805b (2006)).

[30] 1. Reasonable procedures were in place for determining that the acquisition concerned persons reasonably believed to be located outside the United States; 2. The acquisition did not constitute electronic surveillance (i.e., it did not involve solely domestic communications); 3. The acquisition involved obtaining the communications data from or with the assistance of a communications service provider who had access to communications; 4. A significant purpose of the acquisition was to obtain foreign intelligence information; and 5. Minimization procedures outlined in the FISA would be used. *Id.*

[31] Protect America Act of 2007, Pub. L. No. 110-55, § 3, 121 Stat. 552 (Aug. 5, 2007) (amending FISA § 105B(c), codified at 50 U.S.C. § 1805c (2006).

grant the order.[32] Intended to operate for six months, the PAA gave retroactive immunity to service providers to insulate them from civil liability.[33]

Congress continued the PAA until February 17, 2008,[34] eventually replacing it with a more permanent measure: the FISA Amendments Act (FAA).[35] Consistent with this statute, FISA Section 702 empowers the Attorney General and the Director of National Intelligence jointly to authorize, for up to one year, "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[36] FISC annually reviews the certification for the order, to which certain limitations apply.[37] The FAA also brought the targeting of U.S. persons overseas, previously addressed via

---

32 Protect America Act of 2007, Pub. L. No. 110-55, § 4, 121 Stat. 552 (Aug. 5, 2007) (amending FISA § 105C). Twice a year the Attorney General would be required to inform the Intelligence and Judiciary Committees of the House and Senate of incidents or noncompliance with the directive issued by the Attorney General or Director of National Intelligence, incidents of noncompliance with FISC-approved procedures, and the numbers of certifications or directives issued during the reporting period. *Id.*

33 Protect America Act of 2007, §6.

34 Various bills were proposed in the interim. *See, e.g.*, FISA Amendments Act of 2008, S. 2248, 110th Cong. (2007).

35 FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (July 10, 2008).

36 "Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons," Foreign Intelligence Surveillance Act, Pub. L. No. 110-261, § 702, 122 Stat. 2436, codified at 50 U.S.C. § 1881(a) (2006). Except as otherwise noted, section 702 mirrors the definitions adopted in FISA for the terms "agent of a foreign power," "foreign intelligence information," "foreign power," and "person.".

37 Five limitations apply to the order issued by the AG and DNI: first, it "may not intentionally target any person known at the time of acquisition to be located in the United States." 50 U.S.C. § 1881b(1) (2006). Second, it "may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States." § 1881b(2). Third, it "may not intentionally target a United States person reasonably believed to be located outside the United States." § 1881b(3). Fourth, it "may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." § 1881b(4). Fifth, the collection of such information "shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States." § 1881b(5). In exigent circumstances, the Attorney General and the DNI may authorize an immediate acquisition under Section 702; however, they must then submit a certification to the FISC as soon as practicable, but in no event later than seven days after they determined the existence of such exigent circumstances. § 1881b.

Section 2.3 of Executive Order 12333, within FISA, providing greater protections for U.S. persons.[38]

B. *Reform Efforts*

The Snowden releases in June 2013 *et seq.* set off a storm of criticism of the NSA's use of its authorities under FISA and the FAA.[39] Forced on the defensive, the Obama Administration responded by declassifying FISC orders, targeting and minimization procedures, and other documents.[40] Freedom of Information Act litigation initiated by the Electronic Frontier Foundation contributed further to the amount of information in the public domain, resulting during autumn 2013 in the monthly release of previously classified materials.[41]

Cases challenging the legality of these programs are working their way through the courts. Some, directed at FISC, seek to obtain more information about the programs currently underway.[42] Others focus

---

[38] The FAA required, for instance, that the government adopt targeting and minimization procedures for review by FISC. The minimization procedures, in particular, restrict handling information concerning U.S. persons incidentally acquired under Section 702—including the retention and dissemination of such information. Foreign Intelligence Surveillance Act, Pub. L. No. 110-261, § 702, 122 Stat. 2436, codified at 50 U.S.C. § 1881(a) (2006).

[39] For a relatively complete list of key media reports and the Administration's response, see *NSA Documents Released to the Public Since June 2013*, ACLU, https://www.aclu.org/nsa-documents-released-public-june-2013.

[40] Documents declassified by the Administration (both voluntarily and as a result of FOIA litigation) are located at Office of the Director of National Intelligence, *IC on the Record*, *available at* http://icontherecord.tumblr.com/.

[41] The Section 215 documents were released in three batches on September 10, 2013, October 28, 2013, and November 19, 2013. They are archived at Electronic Frontier Foundation (EFF), Transparency Project, *Section 215 of the USA PATRIOT Act*, located at https://www.eff.org/foia/section-215-usa-patriot-act. Further FOIA disclosures from EFF lawsuits related to Section 702 and an opinion of FISC from Oct. 3, 2011, which were released Aug. 21, 2013, are located at https://www.eff.org/foia/fisc-orders-illegal-government-sureveillance.

[42] *See, e.g.*, ACLU's Foreign Intelligence Surveillance Court Motion, No. Misc. 13-02 (FISA Ct. 2013); Yahoo's Foreign Intelligence Surveillance Court Motion, No. Misc 13-05 (FISA Ct. 2013) (challenging the classification of secret court documents); Google's Foreign Intelligence Surveillance Court Motion, No. Misc. 13-03 (FISA Ct. 2013); Microsoft's Foreign Intelligence Surveillance Court Motion, No.Misc. 13-04 (FISA Ct. 2013) (challenging the classification of secret court data); Facebook's Foreign Intelligence Surveillance Court Motion, No. Misc. 13-06 (FISA Ct. 2013); Yahoo's second Foreign Intelligence Surveillance Court Motion, No. Misc. 13-05 (FISA Ct. 2013); LinkedIn's

on the statutory and constitutional questions.[43] It appears that, for now, the Supreme Court is content to let the cases work their way through the lower courts.[44] It is too early to tell how these suits will progress—not least because of difficult issues related to standing, jurisdiction, and Supreme Court precedent. What is clear is that the programs are highly contentious, with the circuits, just nine months into the process, already divided.[45]

Many observers suggest that the best solution to the lack of clarity surrounding the intelligence community's authority to use new and emerging technologies to collect digital information is to amend the current statutory framework governing foreign intelligence and international counterterrorism investigations. Towards these ends, in 2013 Congress held numerous hearings,[46] and members of both

---

Foreign Intelligence Surveillance Court Motion, No. Misc. 13-07 (FISA Ct. 2013); SCLU's second Foreign Intelligence Surveillance Court Motion, No. Misc. 13-08 (FISA Ct. 2013); ProPublica's Foreign Intelligence Surveillance Court Motion, No. Misc. 13-09 (FISA Ct. 2013).

43 *See, e.g.*, Klayman v. Obama, No. 13-0881, 2013 WL 6598728 (D.D.C. 2013) (challenging the Verizon Section 215 order); Klayman v. Obama, No. 13-0851, 2013 WL 6571596 (D.D.C. 2013) (challenging the NSA's PRISM surveillance program conducted under FISA Section 702); ACLU v. Clapper, No. 13-CV-3994 (S.D.N.Y. Oct. 10, 2013) (challenging the Verizon Section 215 order); Smith v. Obama, No. 2:13-CV-00257 (D. Idaho 2013) (challenging the Verizon Section 215 order); Elec. Privacy Info. Ctr. Petition for a Writ of Mandamus, No. 13-58, (U.S. 2013) (challenging the Section 215 Verizon order); First Unitarian Church v. Nat'l Sec. Agency, No. 13-3287 (N.D. Cal. 2013) (challenging electronic surveillance).

44 *See, e.g., In Re* Electronic Privacy Information Center, No. 13-58 (U.S. 2013) (denying petition for a writ of mandamus).

45 *Compare, e.g.*, ACLU v. Clapper, No. 13-CV-3994 (S.D.N.Y. Oct. 10, 2013) (Judge Pauley rejection of government's argument that plaintiffs lack standing, rejection of plaintiffs' claims under the Administrative Procedure Act; acceptance of government statutory construction, and determination that Smith v. Maryland controls for Fourth Amendment purposes) *with* Klayman v. Obama (Klayman I), No. 13-0881 (D.D.C. 2013); Klayman v. Obama (Klayman II), No. 13-0851 (D.D.C. 2013), *available at* https://www.documentcloud.org/documents/901810-klaymanvobama215.html.

46 *See, e.g., Senate Judiciary Committee Hearing on FISA*, 113th Cong. (Dec. 11, 2013); *Senate Judiciary Committee Hearing on Continued Oversight of U.S. Government Surveillance Authorities*, 113th Cong. (Dec. 10, 2013); *Senate Judiciary Committee Hearing on NSA Spying*, 113th Cong. (Nov. 21, 2013); *Senate Judiciary Committee Hearing on Transparency Issues*, 113th Cong. (Nov. 13, 2013); *House Intelligence Committee Hearing on FISA/NSA Program*, 113th Cong. (Oct. 29, 2013); *Senate Judiciary Committee Hearing*, 113th Cong. (Oct. 2, 2013); *Senate Intelligence Committee Hearing*, 113th Cong. (Sept. 26, 2013) (note classified/public sessions); *Nomination of J. Patrick Rowan to be Assistant Attorney General for National Security: Hearing of the Senate Select Committee on Intelligence*, 110th Cong. (Sept. 25, 2008) (discussing Section 702); *Senate Judiciary Committee Hearing on NSA surveillance*, 113th Cong. (July 31, 2013);

Houses introduced dozens of bills centered on FISA reform.[47] Congress has begun 2014 in much the same manner.[48]

As these reform efforts have gained momentum, the Obama Administration has indicated a willingness to amend the current law. In September 2013 the President appointed a Review Group on Intelligence and Communications Technologies.[49] Their final report,

---

How Disclosed NSA Programs Protect Americans and Why Disclosure Aids our Adversaries: House Permanent Select Committee on Intelligence, 113th Cong. (June 18, 2013) (testimony of Gen. Keith Alexander, Deputy Atton'y Gen. James Cole, NSA Deputy Dir. John Chris Inglis, FBI Deputy Dir. Sean Joyce, General Counsel Office of the Director of National Intelligence Robert Litt); *House Judiciary Committee Hearing on NSA Programs*, 113th Cong. (July 17, 2013); *Senate Appropriations Committee Hearing, 113th Cong.* (June 12, 2013) (testimony of Gen. Keith Alexander, Acting Deputy Homeland Security Secretary Rand Beers; Acting Deputy Commerce Secretary Patrick Gallagher, Director of the National Institute of Standards and Technology; Richard McFeely, Exec. Asst. Dir. of the Fed. Bureau of Investigation's Criminal, Cyber, Response and Services Branch).

47 For comprehensive reform bills, *see, e.g.*, USA Freedom Act, S.1599; FISA Improvements Act of 2013, S. 1631, 113th Cong. (2013); FISA Accountability and Privacy Protection Act of 2013, S.1215, 113th Cong. (2013); LIBERT-E Act, H.R. 2399, 113th Cong. (2013); A bill to modify the Foreign Intelligence Surveillance Act of 19789, S.1182, 113th Cong. (2013); Restore Our Privacy Act, S. 1168, 113th Cong. (2013); Fourth Amendment Restoration Act of 2013, S.1121, 113th Cong. (2013); Relevancy Act, H.R. 2603, 113th Cong. (2013); Surveillance State Repeal Act, H.R. 2818, 113th Cong. (2013); Telephone Surveillance Accountability Act of 2013, H.R. 2684, 113th Cong. (2013); Freedom and Privacy Act of 2013, S. 1701, 113th Cong. (2013). For bills addressing FISC reform *see, e.g.*, FISA Court Judge Selection Reform Act of 2013, S.1460, 113th Cong. (2013); FISA Court Reform Act of 2013, S.1467, 113th Cong. (2013); Presidential Appointment of FISA Court Judges Act, H.R. 2761, 113th Cong. (2013); FISA Court Accountability Act, H.R. 2586, 113th Cong. (2013); Privacy Advocate General Act of 2013, H.R. 2849, 113th Cong. (2013); FISA Court in the Sunshine Act of 2013, H.R. 2440, 113th Cong. (2013). For bills covering other aspects of FISA reform *see, e.g.*, Ending Secret Law Act S.1130/H.R. 2475, 113th Cong. (2013); NSA Accountability Act, H.R. 3070, 113th Cong. (2013); Government Surveillance Transparency Act of 2013, H.R. 2736, 113th Cong. (2013); Surveillance Order Reporting Act of 2013, H.R. 3035, 113th Cong. (2013); Surveillance Transparency Act of 2013, S.1452, 113th Cong. (2013); National Whistleblower Appreciation Day, S. Res. 202, 113th Cong. (2013).

48 *See, e.g., Senate Judiciary Committee Hearing on the Report of the President's Review Group on Intelligence and Communications Technologies*, 113th Cong. (Jan. 14, 2014); *Senate Intelligence Committee Hearing on National Security Threats*, 113th Cong. (Jan. 29, 2014) (discussing section 215 and raising concerns about erroneous or misleading statements from government officials during previous hearings on NSA surveillance); *House Judiciary Committee Hearing on Examining Recommendations to Reform FISA Authorities*, 113th Cong. (Feb. 4, 2014); *Senate Judiciary Committee, Hearing on Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime*, 113th Cong. (Feb. 4, 2014); *House intelligence Committee, Hearing on World Wide Threats*, 113th Cong. (Feb. 4, 2014).

49 Press Release, Director of National Intelligence, DNI Clapper Announces Review Group on Intelligence and Communications Technologies, Aug. 12, 2013, *available at*

issued in December 2013, made forty-six recommendations that incorporated a series of significant statutory reforms—including, *inter alia*, an end to the current bulk collection of metadata, the insertion of a constitutional advocate during FISC deliberations, and new limits on and reporting requirements for government applications under and use of FISA sections 215, 402, and 702.[50] The Review Group recommended that future access to metadata be mediated by third parties, with telecommunications providers, or other entities, retaining the information, to which access could be granted only through specific orders from FISC.[51]

In December 2013, in hearings before the Senate, the Deputy Attorney General, the Director of the NSA, and the NSA's General Counsel issued a joint statement supporting limited reform of the current system.[52]

The following month, the President issued a new Presidential Policy Directive (PPD-28), laying out the current principles guiding SIGINT, such as the integration of privacy and civil liberties considerations in the collection of intelligence, limits on the collection of commercial information and trade secrets, and the tailoring of SIGINT to areas where the information is not otherwise available.[53]

---

http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/909-dni-clapper-announces-review-group-on-intelligence-and-communications-technologies. Members of the Review Group included Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter Swire. The original press release called it the "*Director of National Intelligence* Review Group on Intelligence and Communications Technologies," with a directive to report to the President by December 15, 2013; However, the final report, placed on the White House web site, is entitled "Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies." REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [hereinafter REPORT OF THE PRESIDENT'S REVIEW GROUP].

50 REPORT OF THE PRESIDENT'S REVIEW GROUP, *supra* note 49, at 24-30.

51 *Id.*

52 *See, e.g., Senate Judiciary Committee Hearing on Continued Oversight of U.S. Government Surveillance Authorities*, 113th Cong. (Dec. 11, 2013) (testimony of Deputy Attorney General James M. Cole, Director Keith B. Alexander and General Counsel Robert S. Litt), *available at* http://www.justice.gov/iso/opa/dag/speeches/2013/dag-speech-131211.html (stating, "we would be open to discussing legislation authorizing the FISA Court to appoint an amicus, at its discretion, in appropriate cases, such as those that present novel and significant questions of law and that involve the acquisition and retention of information concerning a substantial number of U.S. persons.").

53 Presidential Policy Directive 28, 2014 DAILY COMP. PRES. DOC. 2, §1 (Jan. 17, 2014), *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

The document restricts the use of bulk SIGINT data.[54] It draws attention to the policies and procedures in place with regard to minimization (both dissemination and retention of personal data), data security and access, data quality, and oversight.[55] PPD-28 announced the appointment of a Privacy and Civil Liberties official to assist key parties in their development of policies and procedures, as well as a coordinator for International Diplomacy to serve as a point of contact with foreign governments wishing to raise concerns about U.S. intelligence gathering.[56]

In his speech accompanying issuance of the directive, the President stated his intent to "reform the programs and procedures in place to provide greater transparency to our surveillance activities and fortify the safeguards that protect the privacy of U.S. persons."[57] For the bulk collection program, this meant ordering a transition to end it as it currently exists, and establishing an alternative collection structure—potentially along the lines of that recommended by the Review Group. To facilitate a transfer to a new system, the President instructed the intelligence community to develop options for a new approach, with a report due back to the President prior to FISC's reauthorization consideration March 28, 2014.[58]

The President's remarks and issuance of PPD-28 minimized but did not eliminate the impact of the Privacy and Civil Liberties Oversight Board (PCLOB) Section 215 report, which was slotted for publication the following week.[59] That report made clear that the

---

[54] *Id.*, at § 2 (directing that the data be used "only for the purposes of detecting and countering: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section.").

[55] *Id.* at § 4.

[56] *Id.*

[57] Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), *in* WASH. POST, Jan. 17, 2014, http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html.

[58] *Id.*

[59] PCLOB is an independent, bipartisan entity established by statute whose members are appointed by the President. *See* Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 801(a), 121 Stat. 266, 352-58 (2007).

PCLOB considered the bulk collection of metadata to be illegal as both a statutory and a constitutional matter. The 238-page document called for an end to current program. Two of the board's five members (Rachel L. Brand and Elisebeth Collins Cook, both of whom served in the Department of Justice during the George W. Bush Administration) supported modifications to the program to take account of privacy concerns. The three remaining members (David Medine, who was a Federal Trade Commission official during the Clinton Administration; James X. Dempsey, a public policy specialist at the Center for Democracy and Technology; and Patricia M. Wald, a former federal appeals court judge nominated by President Jimmy Carter), considered it necessary to end the program altogether.[60]

Four days before the deadline, President Obama announced that, notwithstanding a further, 90-day extension of the program, he planned to ask Congress to end bulk collection altogether.[61] In its place, telephone companies will retain the records for the usual amount of time, with the NSA only having access to particular records with FISC approval.[62]

The President's proposal goes some way towards meeting widespread criticism of the Section 215 program. It does not, however, address either all of the critiques, nor does it affect the programs that continue under Section 702.[63] Part of the problem is that the

---

[60] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 168-170, 208-218 (Jan. 23, 2014), *available at* http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf [hereinafter PCLOB REPORT].

[61] Charlie Savage, *Obama to Call for End to NSA's Bulk Data Collection*, N.Y. TIMES, Mar. 24, 2014, http://www.nytimes.com/2014/03/25/us/obama-to-seek-nsa-curb-on-call-data.html?_r=0.

[62] *Id.*

[63] *See, e.g.*, *Foreign Intelligence Surveillance Act Reform*, ELECTRONIC PRIVACY INFORMATION CENTER, http://epic.org/privacy/terrorism/fisa/reform/ (last visited Feb. 19. 2014); Jennifer Grannick, *Reforming FISA: A Critical Look at the Wyden/Udall Proposal and Foreign Surveillance,* CENTER FOR INTERNET AND SOCIETY, STANFORD LAW SCHOOL, http://cyberlaw.stanford.edu/publications/reforming-fisa-critical-look-wydenudall-proposal-and-foreign-surveillance; Orin Kerr, *A Proposal to Reform FISA Court Decisionmaking*, THE VOLOKH CONSPIRACY (July 8, 2013), http://www.volokh.com/2013/07/08/a-proposal-to-reform-fisa-court-decisionmaking/; David Cole & Marty Lederman, *Data-Mining, Section 215, and Regulating the Government's Use of Stored Data: the Overlooked, but More Important, Question about NSA Surveillance*, JUST SECURITY (Dec. 23, 2013), http://justsecurity.org/2013/12/23/review-group-intelligence-communications-technologies-bulk-data-collection-section-215/. *See generally* Category Archives: FISA: Reform, LAWFARE BLOG, http://www.lawfareblog.com/category/fisa/fisa-

conversation has proceeded in a piecemeal fashion. The president's proposal will thus become yet another bill for Congress to consider. What has been missing from the discourse is a comprehensive framework for how to think about potential reforms.[64]

If ever there were a time to re-think how to approach foreign intelligence gathering in a blue-skies fashion, that time is now. Technology has radically altered the landscape from both a threat perspective and from the vantage of privacy and civil liberties. A fragmented approach risks ignoring the potential effects of alterations in the law and opportunities to create a sustainable structure. In constructing such an approach, the first step is to consider how new and emerging technologies have altered the environment in which we now operate. This fundamentally shifts the conversation from a historically-laden approach to one that begins from a different point of analysis: namely, the technologies that now dominate the electronic communications sphere.

III. THE IMPACT OF TECHNOLOGY ON THE INFORMATION RANGE AVAILABLE

The evolution of technology has had a profound impact on how information is generated, transferred, and stored. New types of information are now available. Novel analytical tools allow for the generation of deeper insight into traditional and emerging forms of information. Technology has also affected the geographic assumptions underlying traditional foreign intelligence gathering (i.e., that a sharp line can be drawn between domestic and international information flows, with heightened protections afforded the former).

---

reform/#.UsGp0I5xKPc (highlighting posts by Lauren Bateman, Benjamin Wittes, Raffaela Wakeman, Matt Danzer, Wells Bennett, Peter Margulies, Jack Goldsmith, Tim Edgar, Joel Brenner, Sean Mirski, and others on the topic).

64 *But see* David Kris, *Thoughts on a Blue-Sky Overhaul of Surveillance Laws: Introduction*, LAWFARE BLOG (May 18, 2013), http://www.lawfareblog.com/2013/05/thoughts-on-a-blue-sky-overhaul-of-surveillance-laws-introduction/#.UsG0H45xKPc; David Kris, *Thoughts on a Blue-Sky Overhaul of Surveillance Laws: Challenges*, LAWFARE BLOG (May 19, 2013), http://www.lawfareblog.com/2013/05/thoughts-on-a-blue-sky-overhaul-of-surveillance-laws-challenges/#.UsG0Y45xKPc; David Kris, *Thoughts on a Blue-Sky Overhaul of Surveillance Laws: Approach*, LAWFARE BLOG (May 20, 2013), http://www.lawfareblog.com/2013/05/thoughts-on-a-blue-sky-overhaul-of-surveillance-laws-approach/#.UsGzi45xKPc (3-part blog written prior to the Snowden releases, looking at FISA reform, considering potential challenges to alterations to the current regime, and contemplating possible future approaches).

Overlaying the traditional design has been the creation of additional protections afforded to U.S. persons. The problem is that this approach assumes that the identity of the individual (a) is known; and (b) can be closely aligned with the targeted information. New technologies, however, allow for identity masking and anonymity, as well as for the existence of significant amounts of information dissociated at the front end from individual targets.

In considering potential changes to FISA, it is necessary to first consider how one should think about new and emerging forms of information, and the method by which such information is generated, transmitted, and stored.

A. *Types of Information*

Consider first different types of information. At the most general level, over the past four decades, the law has recognized three principal areas: content, personally-identifiable information (PII), and business records (including, *inter alia*, banking and financial records). These categories have been provided with different levels of protection.

The Supreme Court, for example, has traditionally applied a higher level of protection to content and, in the context of third party doctrine, a lower level of protection to customer records held by companies. Accordingly, traditional FISA created a more stringent regime for electronic communications or physical searches, wherein content would be obtained, and a lower level of protection for the use of pen registers and trap and trace devices.

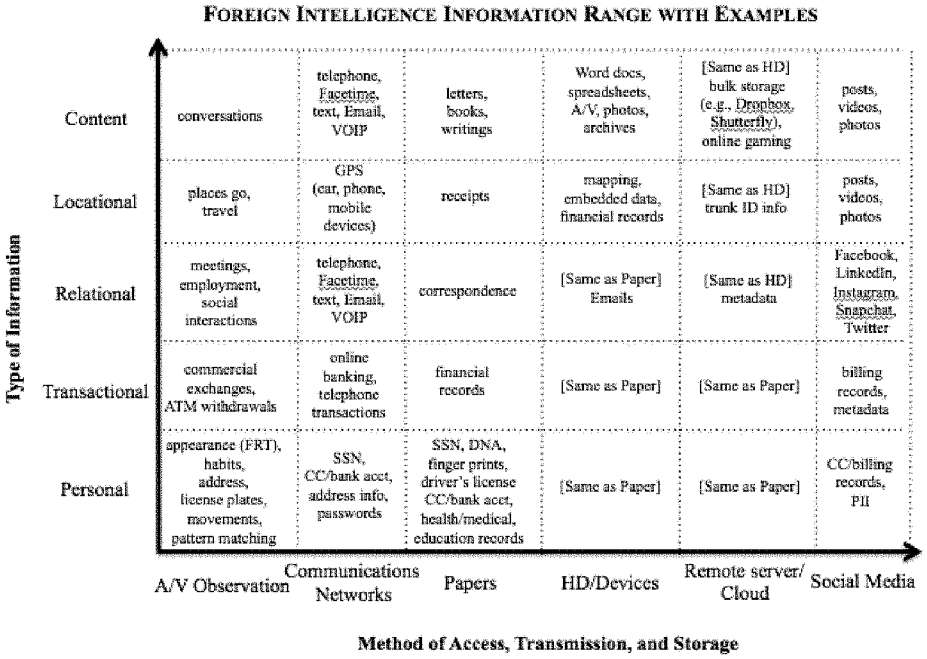
As new technologies have emerged, particularly in a post-9/11 environment, there have been efforts to apply the rules accompanying these categories to new areas. Developed in a different context, though, such statutory requirements may be ill suited to the task. As a result, institutional design may fail, courts may be unable to monitor implementation, Congressional oversight may be lacking, and civil liberties and privacy protections carefully considered in a different context may be bypassed. Continued reliance on these categories also risks masking the impact of emerging technologies on the evolution of each category, as well as preventing recognition of the expansion in the different types of information available.

In light of the current state of technology, it is thus worth considering at least five categories of information that have emerged: personal, transactional, relational, geolocational, and content-based. (See *Figure 1*) A brief discussion helps to illustrate the distinction between these areas.

The first category, personal information, relates to a single individual whose identity can be obtained from the information itself,

or from that information and other information that is in the possession of, or is likely to come into the possession of, the person controlling the information. Traditionally this category has included information such as one's social security number, home address, credit card number, health or medical records, insurance information, and educational records. New technologies, however, have extended this category to include areas like biometric identification markers (e.g., facial recognition, DNA, and iris patterns), habit identification, and pattern matching.

Figure 1



The second category, transactional information, incorporates commercial transactions—i.e., the process of buying or selling something. It suggests a contractual relationship between two or more entities in which goods, services, or money are passed from one entity to another. Historically, this category was limited to banking or financial records or the purchase of property—and, again, differing levels of protection were provided, particularly as it was extended to areas like billing records. But transactional information also includes contractual agreements between entities and records pertaining thereto.

The third category, relational information, has emerged as an independent area as technology related to social network analysis has

evolved. Using both visual and mathematical tools, new technologies allow individuals to map and to analyze various types of flows between people, groups, organizations, geographic regions, computers, URLs, and other connected entities. Relational information gives insight into not just the existence of connections between individuals, but their various roles and groupings within a network—i.e., who are the key connectors, leaders, bridges, and isolates, where the key clusters are and who comprises them, who is in the core of the network, and who is on the periphery. Social network analysis yields additional insight into the distribution of resources (both material and nonmaterial), and potential constraints on individual actions.[65]

The fourth category, locational information, identifies the specific physical location of an object or an individual. It thus relates to the geography of the real world. Geolocational data in particular has come to be associated with technologically-enhanced methods of ascertaining physical placement (e.g., radar, GPS devices in automobiles or mobile phones, or internet connections). This category also incorporates the more traditional mode of ascertaining individuals' locations—i.e., the simple observation of individuals in public space.[66]

The fifth category, content, is perhaps the most traditional category in its close association with both the First and Fourth Amendments. Technology, however, has expanded the range of materials that may provide what can be considered substantive information. At the broadest level, content includes the *substance* of communications, writings, and other materials. As a form of communication, it conveys information through the exchange of ideas, thoughts, or other information, such as through speech, writing, or symbolic representations. It incorporates media content as well, such as pictures, videos, auditory files, and writing. It thus relates to the nature of individual experience.

---

[65] For further discussion *see* STANLEY WASSERMAN AND KATHERINE FAUST, SOCIAL NETWORK ANALYSIS (1994).

[66] Efforts to address the collection of this information have been introduced into Congress, but no laws have yet been passed. *See, e.g.*, Geolocational Privacy and Surveillance Act, S. 639, 113th Cong. (2013); *see also* H.R. 1312, 113th Cong. (2013); Geolocation Privacy and Surveillance Act, S. 1212, 112th Cong. (2011), *see also* Geolocation Privacy and Surveillance Act, H.R. 2168, 112th Cong. (2011) (sponsored by Sen. Ron Wyden and Rep. Jason Chaffetz in the House and Senate respectively). Online Communications and Geolocation Protection Act, H.R. 983, 113th Cong. (2013) (introduced by Reps Zoe Lofgren (D-CA), Ted Poe (R-TX), and Suzan DelBene (D-WA)). Location Privacy Protection Act of 2012, S. 1223, 113th Cong. (2012) (introduced by Sen. Al Franken (D-MN), passed the Senate Judiciary Committee in Dec. 2012).

Each of these categories has privacy interests associated with it that are particular to that type of information. This suggests that consideration of each category, *sui generis*, may be necessary to construct the most appropriate structures to protect such privacy interests. An added layer of complexity here is that the manner in which such information presents in each category—i.e., the way it is accessed, transmitted, or stored—differs.

B. *Method of Access, Transmission, and Storage*

Each of the different forms of information (personal, transactional, relational, locational, and content) may be accessed, transmitted, and stored in different ways. Some of these may be non-digital, such as simply observing another's actions or reading a hand-written letter. Others, such as accessing information held on a server, may be technology-dependent. Simply extending the existing rules from hard copy to hard drives, though, misses the enhanced privacy implications of greater amounts of information and advanced back-end analysis.[67] Six categories here deserve notice: audio/visual (AV) observation; communications networks; papers; hard drives (HD) and device-specific storage; remote server/cloud technologies; and social media. (See *Figure 1*)

The first category, A/V observation, is one of the most traditional ways in which information is accessed. Under this approach, information is obtained by observing a particular target or entity's actions. Traditional modes of information collection in this area still exist—this is the realm of placing a tail on a suspect in the law enforcement world, or of HUMINT in the intelligence community. The key point here is that technology has expanded the ways in which one may be able to observe such actions. Electronic bugs represented one of the early expansions. Placed in an individual's office or home, such devices allow investigators or analysts to hear conversations that are occurring within, thus giving them access to the content of communications. *Katz* dealt with such an "amplifying device," attached to the outside of a phone booth. The Court recognized at the

---

[67] For purposes of this paper, I understand data in a manner consistent with the Data Protection Act, that is, information which: "(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or (e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)." Data Protection Act, 1998, c. 29 (U.K.).

time that new technologies applied to traditional areas could have a deeper impact on the right to privacy.

Other types of technologies are similarly relevant to enhanced A/V observation, and they cross informational categories. CCTV, for instance, may allow for remote surveillance even where the information obtained is not recorded. This extends beyond content information to include locational data: individuals may be followed in public space via traffic cameras, surveillance equipment on drones, satellite cameras, or other technologies. Such tracking may similarly reveal meetings, actions in the workplace, and social interactions—all forms of relational information. Observations of commercial exchanges, such as individuals shopping or withdrawing money from the ATM, represent transactional information. And in the realm of personal information, A/V observation may track individuals by appearance (e.g., using facial recognition), or by license plate [e.g., via automatic license-plate recognition (ALPR) or car plate recognition (CPR) systems]. Such tracking through public space may identify individuals' habits, their home address, their movements, and common patterns in which they engage.[68]

The second category, communications networks, incorporates wire, cable, and satellite communication systems. This is the realm of electronic surveillance—which was one of the central areas addressed by FISA in 1978. The purpose was to provide a heightened level of protection for the content of individuals' communications. But technology has progressed significantly beyond the telephone and wire communications originally considered. Communications networks may be accessed via telephones, computers, or other devices that link up to the Internet. Content information may be conveyed through telephone conversations, FaceTime, texts, emails, or voice over Internet protocol (VOIP).

Much more than content is now involved in information carried through communications networks. Locational data, such as GPS transmissions, may be transferred. Relational data based on telephone and internet content may yield insight into social networks. Transactional information also may be conducted via automated telephone systems: post-cut-through dialed digits (PCTDD) (numbers dialed on a phone once a call has been put through) allow customers to buy airline tickets, transfer money between accounts, and sell stock. In the criminal law realm, efforts have been made to apply PRTT to this area. The problem is that PCTDD also reveals content—suggesting

---

[68] *See* Laura K. Donohue, *Technological Leap, Statutory Gap and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINNESOTA L. REV. 407, 443 (2012).

a deeper privacy interest than mere envelope information.[69] To the extent that automated systems reveal personal data, such as social security numbers (SSN), credit card or bank account numbers, address information, and passwords (such as mother's maiden name, place of birth, name of first pet), personal information is similarly implicated.

Notably, neither of the first two categories (A/V observation and communications networks) record what has historically been considered content. Instead, they record process and movement. Individual A goes to Place 1, then Place 2, and then Place 3; number X dials number Y; or person A uses Credit Card Z. The recording of process and movement *is* what generates information.

Critics of the bulk collection programs point to the generation of information premised on structural connections, and the ability of the government to amass this information in large quantities, at reduced cost, and over extensive periods, to note the significant privacy implication. It may also be prospective, which shifts the question from how to access stored information or already-existing data, to how to control access to information generated in this manner in the future.

The third category, papers, is the one most closely associated with Fourth Amendment jurisprudence—not least because of the wording of the provision itself.[70] Content information located in papers has thus traditionally been afforded the highest level of protection. Since obtaining one's letters, books, and writings, has generally required entry into one's domicile, a warrant, or something approaching a warrant in the realm of foreign intelligence, has typically been required.

FISA, accordingly, includes within its auspices special provisions for physical search that, along with electronic communications (also content-based), are afforded the highest level of protection.

Lines between categories may, of course, be somewhat permeable. The substance of one's papers may demonstrate an individual's location at a particular time, such as via receipts. Relational information may be ascertained from correspondence, and transactional information from financial records. Simultaneously, papers may provide personal information, such as one's health/medical or educational records.

---

[69] In the Matter of Applications of the United States of America for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Information, 515 F.Supp. 2d 325, 335 (E.D.N.Y. 2007).

[70] To wit, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures..." U.S. CONST. amend. IV.

Notably, scientific advances have deepened the type of information that may be found in one's personal papers. DNA technologies, for instance, may reveal a host of information about individuals that was not previously knowable. But minimization procedures have failed to account for the qualitative differences in types of personal information obtained. Instead, they are rather crudely based on whether an individual is a U.S. person or a non-U.S. person.

The digitization of this information has not lessened the privacy interests involved. If anything, its presentation in an analyzable format has deepened the privacy implications. Simultaneously, the increased volume of information means that much more about an individual and his or her movements can be ascertained. Whereas before an individual's prior location might be determined by a receipt, mobile devices now include maps that can be queried for directions and that archive *all* of the places on has travelled. Pictures taken on an iPhone may include embedded data with the precise location at which the image was snapped. To the extent that mobile devices reflect their owner's actions (and not those of others who use or borrow the device), they create a digital map of an individual's movements. Yet the statute—and, indeed, the Court's jurisprudence—has failed to acknowledge this equal, or deeper, privacy intrusion.

As a result, in the fourth category, hard drives and electronic devices, we find varied application of the existing rules. This category encompasses information held in electronic format on individual electronic devices, as well as other forms of local storage, such as memory sticks and stand-alone external hard drives. Content may thus take a number of forms—e.g., documents, spreadsheets, audio/visual files, and new code.[71]

Recent court documents suggest that there is confusion about what level of protection to give to electronic devices in the face of steadily expanding government capabilities. Confronted by requests by the FBI to place malware on a suspect's computer and to access a wide range of information held by the device in the course of an investigation, for instance, district court judges have come out on

---

[71] Early reports about law enforcement use of malware emerged in 2001 with discussion of Magic Lantern. Bob Sullivan, *FBI Software Cracks Encryption Wall*, NBC NEWS.COM (Nov. 20, 2001), *available at* http://www.nbcnews.com/id/3341694/ns/technology_and_science-security/t/fbi-software-cracks-encryption-wall/#.Uz4l04V8qzB. The programs have since become increasingly sophisticated.

different sides of the issue.[72] Network investigative techniques (NIT) allow the FBI to covertly download files, photographs, and stored emails, or even to activate cameras located on computers, allowing the government to obtain real-time images.[73] The privacy interests involved in NIT are substantial. As the Ninth Circuit sitting en banc recognized in *U.S. v. Cotterman* in the context of a border search of a laptop:

> The amount of private information carried by international travelers was traditionally circumscribed by the size of the traveler's luggage or automobile. That is no longer the case. Electronic devices are capable of storing warehouses full of information. The average 400-gigabyte laptop hard drive can store over 200 million pages—the equivalent of five floors of a typical academic library. . . . Even a car full of packed suitcases with sensitive documents cannot hold a candle to the sheer, and ever-increasing, capacity of digital storage.[74]

Pari passu, the amount of information that can be obtained from any individual's laptop is staggering. Recent media reports suggest that the NSA has inserted malware into computer networks, as well as, like the FBI, into individual computers, to collect information.[75]

---

[72] *Compare* Third Amended Search and Seizure Warrant, No. 12-SW-05685 (D. Colo. Dec. 11, 2012); *with* Memorandum and Order, *In Re* Warrant to Search a Target Computer at Premises Unknown, No. 4:13-MJ-00234 (S.D. Tex. Apr. 22, 2013).

[73] Craig Timberg & Ellen Nakashima, *FBI's Search for 'Mo,' Suspect in Bomb Threats, Highlights use of Malware for Surveillance*, WASH. POST, Dec. 6, 2013, http://www.washingtonpost.com/business/technology/fbis-search-for-mo-suspect-in-bomb-threats-highlights-use-of-malware-for-surveillance/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html.

[74] 709 F.3d 952, 964 (2013).

[75] *See, e.g.*, *Violet Blue, NSA Malware Infected Over 50,000 Computer Networks Worldwide*, ZD NET (Nov. 23, 2013), *available at* http://www.zdnet.com/nsa-malware-infected-over-50000-computer-networks-worldwide-7000023537/; Andrea Peterson, *The NSA has its Own Team of Elite Hackers*, WASH. POST, Aug. 29, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/29/the-nsa-has-its-own-team-of-elite-hackers/; Floor Boon, Steven Derix, and Huib Modderkolk, *NSA Infected 50,000 Computer Networks with Malicious Software*, NRC.NL (Nov. 23, 2013), *available at* http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software/; Raphael Satter, *Report: NSA Intercepts Computer Deliveries*, USA TODAY, Dec. 29, 2013, http://www.usatoday.com/story/news/world/2013/12/29/report-nsa-intercepts-computer-deliveries/4244181/.

Simultaneously, the agency has compromised encryption technologies by arranging for secret "back doors" to be built into software, by making secret agreements with private companies, and by using supercomputers to overcome barriers using brute force.[76]

The location of the devices in question, which is one of the traditional ways to think about procuring foreign intelligence, seems to be a minor matter, when compared to the privacy implications of access to such broad swathes of data.

The fifth category, centered on server and cloud technologies, recognizes that the same type of information that may be held on individual devices may be stored on a remote server, such as IBM Cloud, iCloud, Kindle Cloud, or Amazon Cloud. Some companies, such as Dropbox, ZipCloud, SugarSync, and Google Gdrive, offer the ability to store all data remotely, so that the information can be shared and accessed at any time. Other companies, such as Livedrive, Mozy, and BackupGenie, operate primarily as an online backup to individual devices. Yet others, such as MyPCBackup and JustCloud offer both services.

The cloud, though, does more than just offer ways to store information. Cloud computing uses a network of remote servers hosted on the Internet to manage and process data, extending these functions beyond individual hard drives or personal devices. Because of the sophistication of analytical techniques, the amount of storage available, and the potential multi-sourcing of data involved, cloud computing changes what individuals and companies can actually do. It provides an opportunity for users to increase their capacity and to add capabilities without extensive, new investments in infrastructure, software, and personnel. And the market is exploding. As of July 2013, for instance, approximately 30 public companies represented more than $100 billion in market capitalization and $12.5 billion in estimated 2013 revenue.[77]

---

[76] James Ball, Julian Borger, and Glenn Greenwald, *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, THE GUARDIAN, Sept. 5, 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security; Jeff Larson, Nicole Perlroth, and Scott Shane, *Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security*, PRO PUBLICA, Sept. 5, 2013, http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption.

[77] The top 15 cloud computing companies include Jife Software, Demandware, Fleetmatics, RealPage, Dealertrack Technologies, Cornerstone OnDemand, Medidata Solutions, The Ultimate Software Group, Athenahealth, Concur Technologies, ServiceNow, NetSuite, Workday, LinkedIn, and Salesforce.com. Julie Bort, *The 15 Most Valuable Cloud Computing Companies in the World are Worth Way More Than You'd Think*, BUSINESS INSIDER (Jul. 29, 2013), *available at* http://www.businessinsider.com/the-15-most-valuable-cloud-computing-companies-2013-7?op=1.

The same techniques that may be used to exploit hard drives and individual, stand-alone electronic devices may be employed to obtain content, as well as locational, relational, transactional, and personal information, from remote servers. The amount of information available—and insight into—the thoughts and actions of the target may be significantly enhanced—not least because more information can be uploaded and more powerful analytical software may be marshaled in relation to the cloud. In addition, there are some functions, such as online gaming, that are unique to the world of servers in that they take place (in part) on servers located outside the immediate electronic device. Efforts to communicate with others inside the gaming world may be subject to interception with (under traditional foreign intelligence provisions) little or no structure, oversight, or control. Yet this, too, is a form of access to the content of one's communications—an area traditionally afforded the highest, not the lowest, level of protection to ensure that foreign intelligence gathering comports with the Fourth Amendment.

The sixth category, social media, is a form of electronic communication where users can create virtual communities to share information, ideas, personal messages, photographs, videos, and other data. Web sites like Facebook, Twitter, Google+, Instagram, and Snapchat have become a critical form of networking and microblogging. They cross different types of information categories, simultaneously generating content, locational information, and relational information. The companies hosting the sites, in turn, maintain billing records, metadata, and other forms of transactional information, even as they have access to a host of personally-identifiable information about their account holders.

Each of these six categories, as it intersects with the five types of information that now exist, present opportunities for agencies looking to learn information about potential targets. Yet not all information is equal: the substance and techniques employed may yield different levels of value as well as different levels of insight into individuals' private actions, thoughts, and beliefs.

From a value perspective, at one extreme, programs that fail to provide meaningful intelligence in the manner anticipated, may be voluntarily ended by the IC. According to James Clapper, for instance, "[i]n December 2011, the Government decided not to seek reauthorization of the bulk collection of Internet metadata."[78] ODNI

---

[78] Declassification Press Release, *supra* note 1.

explained, "the program was no longer meeting the operational expectations that NSA had for it."[79]

Reliance, however, on the value of a program to the intelligence agency involved for whether it will or will not operate would be misplaced. Individuals who have insight into the program's extent may disagree about its worth. The bulk collection of telephony metadata, has been challenged by individuals on the Senate Intelligence Committee, who have substantial access to the inner workings of the program, on the grounds that it does not yield significant benefits.[80] But not all members of the committee—much less officials in the agencies themselves—agree with that position.[81]

Regardless of how useful a program may be, underlying social, political, and constitutional concerns remain. To the extent that the different categories of information and related access, transmission, and storage yield differing levels of confidential information, different privacy interests come into play. Traditional models, based on, for instance, geography (i.e., whether the object, device, or target is located within US bounds or outside the country), rather miss the point. It is thus crucial to build an expanded understanding of the types of information in question into the statutory framework. These categories fold into the proposed taxonomy, below.

IV. TAXONOMY FOR REFORM

An unsystematic approach to reforming FISA risks masking the ways in which technology has altered the underlying landscape—particularly assumptions built into the statute in 1978. It also imperils the recognition of opportunities to respond more effectively to a

---

[79] *Additional Information on the Discontinued PR/TT Program*, IC ON THE RECORD, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (Dec. 21, 2013), http://icontherecord.tumblr.com/tagged/declassified.

[80] Senator Ron Wyden (D-OR) and Senator Mark Udall (D-CO), for instance, both of whom sit on the U.S. Senate Intelligence Committee, filed an amicus brief in November 2013 in *First Unitarian Church v. NSA*, asserting that they had "reviewed this surveillance extensively and have seen no evidence that the bulk collection of Americans' phone records has provided any intelligence of value that could not have been gathered through less intrusive means." Motion of Senator Ron Wyden, Senator Mark Udall & Senator Martin Heinrich to file a brief Amicus Curiae at 2, First Unitarian Church v. NSA, No. 13-3287 (N.D. Cal. 2013), *available at* https://www.eff.org/document/amici-brief-senators-wyden-udall-heinrich.

[81] *See, e.g.*, Dianne Feinstein, *The NSA's Watchfulness Protects America*, WALL ST. J., Oct. 13, 2013, http://online.wsj.com/news/articles/SB10001424052702304520704579125950862794052.

shifting threat environment, as well as ways in which these new technologies carry with them unique incursions into civil liberties and the Fourth Amendment right to privacy. Minor shifts in statutory construction risk creating imbalance in institutional design. A system, for instance, that is built on placing electronic intercepts on traditional telephone lines may miss the importance of assigning a science and technology expert to FISC in order to help the court to understand new and emerging technologies. Similarly, geographic emphasis may fail to take account of global information flows.

A systematic re-evaluation of foreign intelligence gathering has not occurred since 1978. Statutory changes implemented in 1995, 1998, 2001, 2006, 2008, and 2011 failed to take a universal approach, instead altering the statute in limited or tangential ways.[82] The most significant changes expanded current sections or added new provisions to the statute—such as the addition of business records in 1998 and their expansion in 2001 to tangible goods, or the inclusion of Sections 702, 703, and 704 in 2008.[83] These amendments did not contemplate ways in which technology is changing how we should think about foreign intelligence gathering writ large. They did not consider the broader statutory design. And, for the most part, they did not explicitly deal with new and emerging technologies.

For these reasons, a comprehensive taxonomy is helpful now for thinking through changes that could be put into place. Where might we start if, in light of current technologies, we were to begin constructing a framework for foreign intelligence from the ground up? This question puts some of the assumptions that undergird FISA back on the table for discussion even as it introduces potentially new approaches.

Structurally, the proposed taxonomy can be thought of in two parts: a front-end and a back-end. The former framework deals with the authority to collect information and the latter the implementation of the authorities—i.e., the manner in which such information is obtained, analyzed and used. Both frameworks sub-divide into two sections that exist in equilibrium: the first deals with the positive grant of authority, and the second with a check on the exercise of such

---

[82] Intelligence Authorization Act of 1995, Pub. L. No. 103-359, 108 Stat. 3423 (1994), Intelligence Authorization Act of 1999, Pub. L. No. 105-272, 112 Stat. 2396 (1998); USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001); USA PATRIOT Additional Authorization Amendments Act of 2006, Pub. L. No. 109-178, 120 Stat. 278 (2006); FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008); FISA Sunsets Extension Act, Pub. L. No. 112-3, 125 Stat. 5 (2011).

[83] *Id.*

powers. The latter thus balances the former, providing a counterpoise to potential authorities.

Although the typology is designed to be cognizant of the need to create avenues for the collection and analysis of foreign intelligence information, as well as the need for protections on the exercise of these authorities, it does not in and of itself take a position on where these lines should be drawn. Instead, the purpose is to highlight the types of provisions that could be taken on board in building a comprehensive framework.

A. *Front-End Framework to Collect Foreign Intelligence Information*

Front-end considerations relate to the acquisition of information. They divide into (1) the manner of collection, and (2) requirements for approval of the authorities thereby created. (See *Figure 2*) The structure thus reflects a positive grant of authority under certain conditions (1), and structures to ensure that the appropriate processes are followed prior to government entities acting on those powers (2). While (2) thus acts primarily as a limitation on (1), it would be too simplistic to say that each category only performs these functions. For there are a number of ways in the sub-divisions in (1) could be constructed to provide checks on the system. Nevertheless, approaching the question in this manner allows for attention to be drawn to the different functions of the relevant entities.

Figure 2
Front-End Framework to Collect Foreign Intelligence Information

Manner of Collection	Requirements for Approval
1. **Type of information** a. Content b. Locational c. Relational d. Transactional e. Personal 2. **Method of access/transmission/storage** a. A/V (immediate observation) b. Communications Technologies c. Paper/tangible goods d. HD/Device e. Server/Cloud Technologies f. Social media 3. **Form in which information is transferred** a. Anonymization and re-identification b. Prior screening by third party 4. **Agency obtaining information** a. Broad institutional design (e.g.,	1. **Entity Approving Collection** a. Executive - agency-internal - agency-external b. Judicial - special court (e.g., FISC) - ordinary Art. III court - Art. I court c. Other (e.g., private industry) 2. **Construction of entity** a. Selection of decision-makers - originating entity (e.g., Circuit division, regional division, etc.) - manner of selection (e.g., President, Chief Justice, SCOTUS, Congress) b. Length/progression of terms (period of years, staggered terms, term limits) c. Adversarial processes

NSA/CYBERCOM division) b. Primary authorization (e.g., FBI, CIA, NSA) c. Concurrences req'd (e.g., AG, NSD) 5. **Target** a. US v. non-US persons b. Foreign powers/agents thereof c. Terrorists (KSTs/Int'l) 6. **Source of information** a. Private industry - data retention requirements and costs - voluntary v. compulsory compliance - data security - litigation risks b. Third party data holders - relationship to gov't, private entities - division of information between entities - data security. - encryption keyholders (internal/external) c. Government agencies d. Non-governmental entities e. International partners - verification of information 7. **Location of information** a. International v. domestic b. Mixed (e.g., cyber) c. Border	- Rights of challenge - Rights of appeal - Third party rights - Constitutional advocate d. Technological expertise 3. **Scope of approval** a. Application format b. Standards (e.g., particularized, RAS) c. Duration d. Renewal requirements 4. Verification a. Third party data holder requirements b. Encryption keyholder requirements 5. **Emergency exceptions** a. Substantive requirements b. Timeline for subsequent approval c. Use of information

1. *Manner of Collection*

The first two considerations in the manner of collection center on the type of information in question and the method of access thereto, as well as the way in which such information is transmitted and stored. Part III of this article has already considered these areas in some depth. A short discussion will help to illustrate how using these demarcations would significantly depart from the current orientation of FISA, which relies on the target and the location of the information, and help to construct a new approach to foreign intelligence.

Consider first the type of information. It may be personal and/or transactional information (e.g., the association of particular credit card numbers or billing records in relation to specific individuals) should be considered in a category apart from relational information, which in turn could be distinguished from locational or content-based information.

In other words, the associated structures may depend upon the type of information being sought. The number and types of entities from whom personal and/or transactional information may be

obtained, the process for obtaining the information, what information may be retained, the manner and length of time of retention, and the use of such provisions would then revolve around the information itself, thus allowing the provisions to be tailored to the specific privacy interest involved.

This approach allows for more careful consideration of the type of information in question. For relational information, for instance, in addition to the threshold issue, perhaps the most important question is how to treat different levels of social connectedness—e.g., it may be a lesser privacy intrusion to obtain information *that* an individual is a member of an organization, than to look at relationships within organizations to consider the role one plays within the entity. Similarly, it may be that there are greater (or fewer) privacy interests in building social networks of geographic regions versus looking at individuals with similar political, economic, or religious subject-matter-interests. The mere observation of individuals' involvement, moreover, may be less intrusive than the digitization of such information and the combination of such data with other information—suggesting heightened privacy protections as one moves outward along the digitization axis (see *Figure 1*).

To the extent that locational information reveals substantive data, perhaps it should be placed within a framework similar to content-based approaches. Again, the outward movement along the digitization axis may trigger further protections as the data changes form or is incorporated into recombinant systems (i.e., systems that combine data with other information that allows the user a greater level of insight into individuals' private lives).

Beyond the first two categories (the type of information, and the method of access, transmission, or storage), the manner of collection may be constructed with reference to five further areas. First, the form in which information is transferred may be considered as part of the front-end collection. The data, for instance, may be anonymized before it is provided to the government agency, with only certain data points meeting a pre-set selection criteria then subjected to re-identification.[84] Alternatively, a third party data-holder may pre-screen the results of any searches. Thus, for instance, if a search returns 400 numbers, those relating to non-concerning entities could be screened out prior to government examination of the data.

Second, contours may be built around access to information based on the agency obtaining the information. This, in turn, has three components: (a) broad institutional design [e.g., deciding to separate

---

[84] *But see* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

NSA/CYBERCOM or requiring civilian personnel to head particular agencies], (b) primary authorization [e.g., authorizing the FBI but preventing the CIA (as in Exec. Order 12333) from engaging in certain activities], and (c) concurrences required [e.g., requiring the Attorney General or the Assistant Attorney General of the National Security Division to sign off on applications to obtain information].

The third consideration is the target about whom information is sought. Traditionally, FISA has focused on U.S. versus non-U.S. persons, presenting higher barriers to collection of information on the former, versus the latter. It has overlaid this with two additional categories—namely, whether individuals are foreign powers or agents thereof, or involved in international terrorism. These categories are decidedly individual, requiring a nexus between the target of the information and the category. Discussion thus may turn on the level of suspicion required to collect information related to a target, for instance requiring a statement of facts supporting reasonable, articulable suspicion. (Note that one would then expect parity between this and the scope of approval, addressed, below).

A fourth, associated area may be the source of the information itself. FISA has only tangentially considered this in relation to business records and, subsequently, tangible goods. But there are numerous sources that could be considered. Private industry may generate and/or store information. Different approaches that could be taken here include possibly introducing data retention requirements, which gives rise to considerations of cost. Data security prior to government access could be statutorily addressed. Attention also could be drawn to voluntary versus compulsory compliance and associated risks of litigation borne by the companies. Alternatively, reform efforts may want to focus on constructing new, third-party data holders, which may be linked in some way either to government or to industry—or to neither. Under this approach, further thought may be given to dividing information between entities for additional protection of data. In this case, the security of the data would also be relevant, as would the potential for introducing yet another third party in the form of encryption key holders—the purpose of which is to divide the process via which the information is accessed.[85] Encryption key holders may also be built into the independent entity holding the data, much like an Inspector General office is part of the institutional framework of a government entity.

Information may also be obtained from other government agencies, in which case interim Memorandum of Understanding,

---

[85] *But see* Scott D. Sagan, *The Problem of the Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security*, 24 RISK ANALYSIS 935 (2004).

standards, and procedures will have to be taken into consideration, or it may be derived from non-governmental entities. If obtained from international partners, further verification of the information may be required. If this is the favored approach, the type of framing used alters. For example, lower levels of reliance may be assumed when information comes from foreign entities, in relation to which the U.S. has limited control, suggesting greater minimization procedures until information is verified. Alternatively, to protect other agencies' missions, it may suggest limiting intra-governmental transfer of information; additionally, in the interests of privacy, it may mean creating higher barriers to obtaining information from a target's employer, requiring a higher showing before a neutral arbiter before obtaining certain records.

The fifth additional area associated with the manner of collection is location. Traditionally, FISA has considered international versus domestic. But the possibility of having a mixed category (e.g., where information flows across borders), or one focused on the border itself may sharpen the analysis.

2. *Requirements for Approval*

Having considered the manner of collection, attention then turns to checks on these authorities in the form of what is required for approval prior to the collection of the information—essentially, the process that must be followed in order for collection to commence. Here, there are four principal considerations: the entity(ies) approving the collection, how that entity is constructed, what the scope of the approval is, and emergency exceptions. Underlying this demarcation is the time-honored understanding that having a neutral arbiter provides an important check on the exercise of authority.

The entity approving collection may be one of three forms. Within the executive branch, it may be internal or external to the intelligence agency that has been authorized to collect the data. In the judicial realm, there are three types of arbiters that may be constructed: a special court (like FISC), an ordinary Article III court, or an Article I court. There may, in addition, be a way to construct a board or independent arbiter from other sources, such as private industry or quasi-governmental organizations.

The construction of the entity itself also offers numerous options. The manner in which decision-makers are selected may include requirements with regard to the originating entity (for instance requiring a division among certain circuits, regions, or types of industry), as well as the manner of selection (e.g., by the President with the advice and consent of the Senate, by the Chief Justice of the Supreme Court, by members of the Supreme Court, by the Appellate

Courts, or by particular committees in Congress). The length of the terms, or their progression (e.g., the period of years, staggered terms, and term limits) may also be considered. Adversarial processes, in turn, may involve rights of challenge to the orders, rights of appeal, third party rights, or the creation of a constitutional advocate, while technological expertise similarly may be built into the statutory design.

The scope of approval contributes further to the potential requirements that must be met prior to acquisition of information. This category highlights the form that the application or request must take, standards that the entity must follow in approving or disapproving of the applications, the duration for which applications may be granted, and the contours of any requirements for renewal.

Although not currently required under the statute, depending upon the final form of data storage and access, it may be desirable to include an additional verification stage—i.e., requirements that must be met by certain actors in verifying that the requesting agency has gone through the appropriate steps. These may apply to third party data holders, such as telecommunications companies, or independent entities established for the purpose of holding the data for intelligence purposes. It may be equally relevant for encryption key holders, prior to allowing access to the information.

A final area to highlight relates to emergency exceptions that could be constructed to take account of national security crises. Three principal areas (substantive requirements, the timeline for subsequent approval, and the subsequent use of information obtained during the exercise of the emergency provisions) provide the focus. Taken together, these various approaches suggest a more comprehensive view of ways to provide access to new types of information.

B. *Back-End Framework to Analyze and Use Foreign Intelligence Information*

Like front-end considerations, a range of categories could be used to explore the construction of a back-end framework centered on implementation of the authorities thereby granted. This framework also divides into two parts, reflective of the positive grant of authority and subsequent checks on the same powers, even as considerations within each category may consider both aspects as well. These realms relate to implementation, on the one hand, and transparency and oversight, on the other. (See *Figure 3*)

Figure 3
Back-End Framework to Analyze and Use Foreign Intelligence Information

Implementation	Transparency and Oversight
1. **Analysis** a. Raw data - type of analysis (e.g., data mining, social network analyses) - levels of analysis (e.g., primary, secondary, tertiary) - requisite standards and processes to be followed b. Recombinant information - substantive (e.g., biometric v. biographic) - programmatic (e.g., Sec. 215/Sec. 702) - source (e.g., intra-agency and inter-agency; government and private databases) c. Verification 2. **Use** a. Minimization b. Judicial processes (e.g., prosecution, use of information as evidence in trial, etc.) c. Consequential actions (e.g., further targeting, watch listing, etc.) 3. **Retention** a. Length of time b. Who holds the information (e.g., NSA, FBI, DNI, CIA) c. How is the information held (e.g., digital v. hard copy, combined with PII or other data v. isolated) d. Access (e.g., which individuals within agency, which agencies, under what conditions) 4. **Transfer** a. To whom b. Restrictions on use, access, and sharing c. Verification	1. **Who reports** a. Agency executing foreign intelligence authorities b. IC entity's Inspector General - Administrative (e.g., NSA, NGA, NRO IGs) - Statutory (e.g., CIA IG, DOJ IG) c. IC entity's privacy officer d. Concurrence entity (e.g., NSD) e. Approval entity (e.g., FISC) f. External Agencies (e.g., ODNI, OMB) g. Entities providing the information to the IC (e.g., private sector, NGOs) h. Independent oversight body (e.g., PCLOB) 2. **What is reported** a. Execution of authorities (e.g., #/range of orders, programs, benefits/rates of success) b. Application under the law (e.g., novel or significant legal interpretations, application to new technologies) c. Noncompliance (willful and non-willful) d. Non-standard (specifically requested) information 3. **To whom report** a. Head of agency executing foreign intelligence authorities b. IC entity's IG or privacy officer c. Concurrence entity d. Approval entity e. External agencies f. Independent bodies (e.g., PCLOB) g. Congressional committees h. Public 4. **Penalties for violations** a. Administrative (e.g., reprimand, loss of security clearance, suspension, termination) b. Civil (e.g., fines) c. Criminal (e.g., prison) 5. **Alternative reporting channels** a. fraud, waste, abuse (programmatic) - path (agency, supervisor, ODNI, Congress) - protections against recrimination b. Public interest (systemic) - external body - criminal defense (*ex post* v. *ex ante*)

1. *Implementation*

Implementation centers on how the authorities granted to the intelligence community are actually used. There are four categories to consider: analysis, use, retention, and transfer. Traditionally, emphasis has only been placed on the second and third areas and, even within these, on only a few components (e.g., minimization procedures and the length of time data is retained). The taxonomy thus allows more careful scrutiny of different aspects of the implementation phase and expands the ways in which Congress could approach each area.

Under analysis, for instance, a new foreign intelligence framework could focus on how raw data is treated. Emphasis on the type of analysis, such as what sorts of data mining or social network analyses can be performed could be considered, as well as levels of analysis (e.g., primary, secondary, and tertiary "hops"). Attention may be drawn to the requisite standards and processes to be adopted prior to progressing from one stage to the next.

Consideration could also focus on what I call "recombinant information"—namely, the combining of information from different sources in a way that generates new knowledge. Attention can be paid to combining substantively distinct information, such as biometric and biographic data. It may center on programmatic combinations. For instance, agencies may want to combine information from different programs run under the same legal authorities (e.g., Section 215), or from programs run under different legal authorities (e.g., Sections 215 and 702). Alternatively, agencies may want to combine databases held in different areas of the agency with databases held outside the agency, or government databases with publicly-available databases. Another consideration in looking at the analysis of the data centers on information verification. This becomes particularly important when subsequent intrusions into civil liberties and individual privacy may flow from the initial analyses. This approach would help to highlight new and emerging ways in which data analysis is progressing.

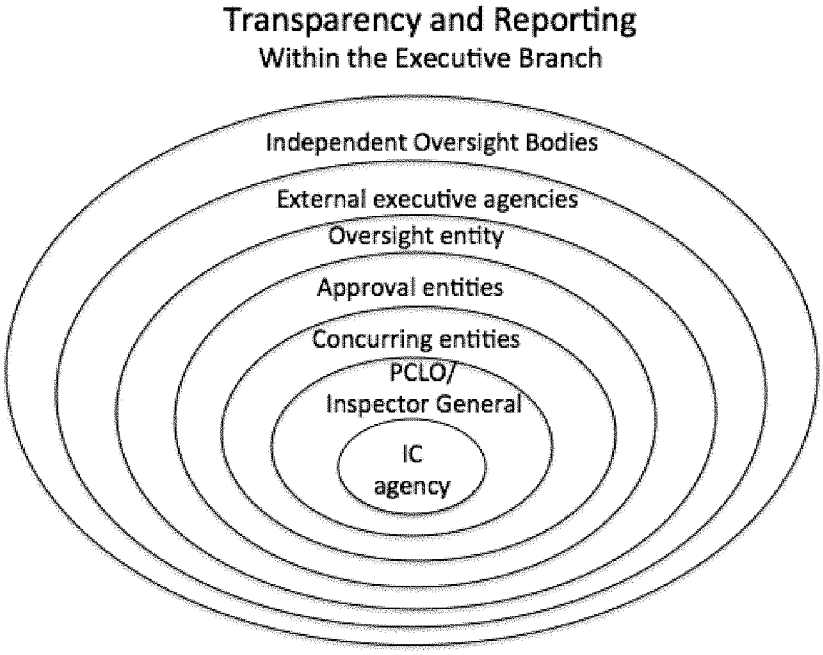
The use of such information also presents an opportunity for statutory construction. Minimization procedures have historically been considered (and still offer) an opportunity for further inspection. But prosecutorial limits, the use of such evidence in trial, and other judicial process-related concerns may be taken on board, as well as the extent to which consequences that follow from initial analyses, such as further targeting or watch listing, raise civil liberties concerns.

Retention has historically been limited to considerations about time, but there are other questions that could also be statutorily addressed. Once *obtained* (and not just at the outset), who should

hold the information? Should it be held by the NSA? The FBI? The CIA? Different government entities have different missions, and so the placement of the data is of consequence. Beyond the entity responsible for the data, how is the information being held? It may be in digital form or hard copy. It may be combined with other data or personal identifiers, or it may be isolated. Additionally, access may be considered—not just who has access within the intelligence agency in question (e.g., on a need to know basis, by level of clearance, or by programmatic assignment), but which other agencies have access to the information as well.

The final consideration relates to transferring the data. This incorporates the recipient of the information, further restrictions on use, access, and sharing, and ways in which the information may be verified in the future.

Figure 4



2. *Transparency and Reporting*

The flip side of the design for implementing the authorities granted to the intelligence community is considering how such use is to be monitored. As with requirements for approval at the front end, this area acts as a counterpoise, balancing the power to collect foreign

intelligence with protections to prevent improper use of the same. It subdivides into five primary considerations: who reports, what is reported, to whom the report is made, penalties for violations, and alternative reporting channels.

The first area, who reports, incorporates entities internal and external to the entity exercising the authorities. A good way to think about this area is in terms of concentric circles. (See *Figure 4*) In the core, the specific agency engaged in foreign intelligence collection may be required to report. One level out, the IC entity's inspector general may be brought on board. Of relevance is the underlying structure of this position—i.e., either administrative (e.g., the current IGs of the NSA, NGIA, and NRO), or statutorily required (e.g., the current IGs of the CIA and DOJ). Additional consideration can be given to reporting requirements to the IC entity's privacy officer. The next ring includes any entities required for concurrence at the front-end application or initiation, such as DOJ's National Security Division. The adjoining circle incorporates any entity required for approval of the intelligence gathering. This may be FISC, or some other entity created for the purpose of addressing the counterpoise to the front-end considerations. The following band includes external agencies, which perform oversight within the executive branch, such as ODNI, or OMB. The abutting loop focuses on entities that provide information to the IC—such as the private sector or NGOs. On the outermost ring we then find independent oversight bodies, such as the PCLOB.

The question of who reports folds then into the second area, which is what is reported. Entities may be required to report on the execution of authorities (e.g., the number and range of orders, programs underway, and benefits or rates of success). They may address how the programs have been applied under the law, detailing novel or significant legal interpretations, or the extension of prior legal analysis to new technologies. Noncompliance requirements (either willful or non-willful) are included here. Finally, of importance will be the manner in which non-standard (specifically requested) information will be handled.

Having looked at who reports and what is reported, the third area to consider is to whom such information is made available. For logical reasons, the potential list of recipients is to some measure co-extent with the entities considered for who makes the report (to ensure access to information necessary for them to fulfill their statutory duties). But there are some differences. Thus, reports may be required under certain circumstances to (a) the head of the agency executing the foreign intelligence authorities, (b) the entity's inspector general or privacy officer, (c) the concurring entity, (d) the approval entity, (e) other executive branch agencies, or (f) independent bodies. In addition, (g) Congress, and (h) the public may also be considered for

receiving reports from the various reporting bodies. While the latter reports would necessarily be unclassified, the reports to the preceding areas [(a)-(g)] may be either classified or unclassified.

Crossing the first three categories are questions related to the burden such reporting may place on the agencies involved, in terms of time, personnel, and money. Special appropriations may be made, for instance, to account for the need to develop new technologies to allow for auditing programs, or to hire additional analysts to act in an internal capacity. Alternatively, consideration of reporting requirements as a whole may help to streamline the overall process.

The fourth consideration in transparency and oversight focuses on what to do about misuse of authorities. Penalties for violations may include administrative measures, such as reprimands, loss of security clearances, suspension, or termination. Civil remedies such as fines may be created, or criminal measures may be attached.

The fifth and final consideration focuses on what to do when the regular reporting channels are not working. How should one conceive of alternative reporting channels? Here, there appear to be two divisions. The first, relating to fraud, waste, and abuse, tends to be programmatic in that it focuses on specific programs in place. Questions to address include (a) the path that individuals concerned about fraud, waste, and abuse should follow (e.g., within the agency, relating to supervisors, going to ODNI, or approaching Congress), as well as (b) protections against recrimination. The second division emphasizes public interest—representing a systemic (not a programmatic) concern about the exercise of foreign intelligence gathering authorities. Here, attention may be paid to the role of external bodies as well as potential criminal defenses available in the event that the matter goes to trial (*ex post* v. *ex ante* considerations).

V. CONCLUDING REMARKS

Public knowledge of PSP has generated widespread calls for FISA reform. Proponents of change point to the general approach adopted by Congress in passing FISA, the statutory language itself, and Fourth and First Amendment constitutional concerns as a basis for introducing alterations.

The trouble with many of the proposals is that they fail to adopt a fresh start to the question of foreign intelligence, instead, looking for fixes to specific problems. The quandary, however, is much bigger than, for instance, the lack of adversarial counsel, or the five year retention of data by the NSA. The problem is that technology has radically altered, and the approach on which FISA rests, centered on targets and geography, is now woefully inadequate for the world in which we now live.

It is for this reason that this Article has sought to look at how technology itself has altered since 1978, in terms of the types of information that are now available (i.e., personal, transactional, relational, locational, and content) and in the methods by which such information can be accessed, transmitted, and stored (namely, observation, communications networks, papers, hard drives and stand-alone devices, remote servers and cloud technologies, and social media).

Using these divisions as a basis for the first part of the front-end framework, the proposed taxonomy builds on them to add considerations related to the form in which such information is transferred, the agency seeking the information, the target about whom information is sought, and the source and location of information. Set against the manner of collection at the front-end, are the requirements for approval. Here, the entity approving the collection, the construction of that entity, the scope of the approval to be granted, potential verification regimes, and exceptions in times of emergency may be considered.

For the back-end framework to analyze and use foreign intelligence information, implementation divides into four primary areas: analysis, use, retention, and transfer. The check on these authorities primarily takes the form of transparency and oversight, which further subdivided into five areas: who reports, what is reported, to whom they report, penalties for violations, and alternative reporting channels.

While the taxonomy does not represent a radical reconception of intelligence collection, it does expand the scope of the current reform efforts addressed in Part II to include the range of potential areas that could be brought on board. In doing so, it builds on the country's experience over the past 36 years even as it recognizes changed circumstances. Although the Article takes no normative position on the specific reforms to be given effect, it clarifies areas critical for discussion and, in so doing, their complex relationship with other elements in the framework. The hope is that the taxonomy may serve as a way to move the conversation forward in developing an approach to foreign intelligence gathering that is cognizant of the need to obtain foreign intelligence, even as it recognizes the changing privacy interests implicated by new and emerging technologies.